3e Technologies International, Inc.
FIPS 140-2
Non-Proprietary Security Policy
Level 2 Validation

3e-519, 3e-525A and 3e-525N

Version 1.1

October 26, 2005

Glossary of Terms

AP	Access Point
CO	Cryptographic Officer
DH	Diffie Hellman
DHCP	Dynamic Host Configuration Protocol
DMG	Dual Mode Gateway
DMZ	De-Militarized Zone
IP	Internet Protocol
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
HTTPS	Secure Hyper Text Transport Protocol
LAN	Local Area Network
MAC	Medium Access Control
NAT	Network Address Translation
PRNG	Pseudo Random Number Generator
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SRDI	Security Relevant Data Item
SSID	Service Set Identifier
TLS	Transport Layer Security
WAN	Wide Area Network
WLAN	Wireless Local Area Network

1. Introduction

1.1 3e-519

This section describes the non-proprietary cryptographic module security policy for 3e Technologies International's wireless gateway product, the 3e-519 Wireless Gateway (Hardware Version 1.0, Firmware Version 3.018.14 and Hardware Version 2.0, Firmware Version 3.0.18.16). This policy was created to satisfy the requirements of FIPS 140-2 Level 2. This section also defines 3eTI's security policy and explains how the 3e-519 meets the FIPS 140-2 security requirements.

The figure below shows the 3e-519 Wireless Gateway.

3e-519 Wireless Gateway

The cryptographic module security policy consists of a specification of the security rules, under which the cryptographic module shall operate, including the security rules derived from the requirements of the standard. Please refer to FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules* available on the NIST website at http://csrc.nist.gov/cryptval/.

1.1.1 Definition

The 3e-519 is a device which consists of electronic hardware, embedded software and strong metal case. For purposes of FIPS 140-2, the module is considered to be a multi-chip standalone product. The 3e-519 operates as either a gateway connecting a local area network to wide area network (WAN) or as an access point within a local area network (LAN). The cryptographic boundary of the 3e-519 is defined to be the entire enclosure of the Gateway. The 3e-519 is physically bound by the mechanical enclosure which is protected by tamper evident tape.

3eTI Gateway software provides the following major services in FIPS mode:

- Wireless 802.11b Access Point functionality (bridging from the wired uplink LAN to the wireless LAN).
- Wireless 802.11b/g bridge functionality
- DHCP service to the local LAN (allows a wired local LAN to exist over the local LAN interface).
- SNMP*
- USB printer services
- Subnet Roaming

* Although SNMP traffic is transmitted encrypted (using DES or AES), for FIPS purposes, it is considered to be plaintext. The reason being, encryption keys are derived from a pass-phrase, which is not allowed in FIPS mode.

1.2 3e-525A

This section describes the non-proprietary cryptographic module security policy for 3e Technologies International's wireless gateway product, the *3e-525A Wireless Gateway* (Hardware Version 1.0, Firmware Version 3.018.14 and Hardware Version 2.0, Firmware Version 3.0.18.16), hereafter known as the 3e-DMG (Dual Mode Gateway). This policy was created to satisfy the requirements of FIPS 140-2 Level 2. This section also defines 3eTI's security policy and explains how the 3e-DMG Wireless Gateways meet the FIPS 140-2 security requirements.

The figure below shows the 3e-525A Wireless Gateways.

3e-525A Wireless Gateway

The cryptographic module security policy consists of a specification of the security rules, under which the cryptographic module shall operate, including the security rules derived from the requirements of the standard. Please refer to FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules)* available on the NIST website at http://csrc.nist.gov/cryptval/.

1.2.1 Definition

The 3e-DMG Wireless Gateway is a device which consists of electronic hardware, embedded software and strong metal case. For purposes of FIPS 140-2, the module is considered to be a multi-chip standalone product. The 3e-DMG gateway operates as either a gateway connecting a local area network to wide area network (WAN) or as an access point within a local area network (LAN). The cryptographic boundary of the 3e-DMG Gateway is defined to be the entire enclosure of the Gateway. The 3e-DMG is physically bound by the mechanical enclosure which is protected by tamper evident tape.

3eTI Gateway software provides the following major services in FIPS mode:

- Wireless 802.11b Access Point functionality (bridging from the wired uplink LAN to the wireless LAN).
- Wireless 802.11b/g bridge functionality
- DHCP service to the local LAN (allows a wired local LAN to exist over the local LAN interface).
- SNMP*
- USB printer services
- Subnet Roaming

1.3 3e-525N

This section describes the non-proprietary cryptographic module security policy for 3e Technologies International's wireless gateway product, the *3e-525N* (Hardware Version 1.0, Firmware Version 3.018.14 and Hardware Version 2.0, Firmware Version 3.0.18.16). This policy was created to satisfy the requirements of FIPS 140-2 Level 2. This section defines 3eTI's security policy and explains how the 3e-525N meets the FIPS 140-2 security requirements.

The figure below shows the 3e-525N.

3e-525N Wireless Gateway

* Although SNMP traffic is transmitted encrypted (using DES or AES), for FIPS purposes, it is considered to be plaintext. The reason being, encryption keys are derived from a pass-phrase, which is not allowed in FIPS mode.

The cryptographic module security policy consists of a specification of the security rules, under which the cryptographic module shall operate, including the security rules derived from the requirements of the standard. Please refer to FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules)* available on the NIST website at http://csrc.nist.gov/cryptval/.

1.3.1. Definition

The 3e-525N is a device which consists of electronic hardware, embedded software and strong metal case. For purposes of FIPS 140-2, the module is considered to be a multi-chip standalone product. The 3e-525N operates as either a gateway connecting a local area network to wide area network (WAN) or as an access point within a local area network (LAN). The cryptographic boundary of the 3e-525N is defined to be the entire enclosure of the Gateway. The 3e-525N is physically bound by the mechanical enclosure which is protected by tamper evident tape.

3eTI software provides the following major services in FIPS mode:

- Wireless 802.11b Access Point functionality (bridging from the wired uplink LAN to the wireless LAN).
- Wireless 802.11b/g bridge functionality
- DHCP service to the local LAN (allows a wired local LAN to exist over the local LAN interface).
- SNMP*
- Subnet Roaming

1.4 Scope

This document covers the secure operation of the 3e-series wireless gateway products, including the initialization, roles and responsibilities of operating the product in a secure, FIPS-compliant manner, and describe the Security Relevant Data Items (SRDIs).

The Gateway has four modes of operations which are listed in the table below:

Mode	FIPS Mode
Gateway Mode (Mode 1)	No
Gateway Mode (Mode 2)	Yes
AP / Bridging Mode (Mode 1)	No
AP /Bridging Mode (Mode 2)	Yes

* Although SNMP traffic is transmitted encrypted (using DES or AES), for FIPS purposes, it is considered to be plaintext. The reason being, encryption keys are derived from a pass-phrase, which is not allowed in FIPS mode.

* Although SNMP traffic is transmitted encrypted (using DES or AES), for FIPS purposes, it is considered to be plaintext. The reason being, encryption keys are derived from a pass-phrase, which is not allowed in FIPS mode.

The Gateway – FIPS mode (Mode 2) and AP/Bridging - FIPS mode (Mode 2) are explained in this document. The other modes cannot be validated by FIPS because they execute applications that use non-FIPS cryptographic algorithms.

In order to enter FIPS mode, select the FIPS 140-2 Mode box on the Operation Mode page of the management GUI. This will force the gateway to return to factory defaults and then the gateway will reboot into FIPS mode. To leave FIPS mode, deselect the FIPS 140-2 Mode box and apply the changes. Once again, the gateway will restore factory defaults and then reboot into non-FIPS mode.

On transition between modes, the system is returned to factory defaults.

2. Roles, Services, and Authentication

The 3e-series supports four separate roles. The set of services available to each role is defined in this section. The 3e-series Gateway authenticates an operator's role by verifying his PIN or access to a shared secret.

2.1 Roles and Services

The 3eTI gateway supports the following authorized roles for operators:

Crypto Officer Role: The Crypto officer role performs all security functions provided by the Gateway. This role performs cryptographic initialization and management functions (e.g., module initialization, input/output of cryptographic keys and SRDIs, audit functions and user management). The Crypto officer is also responsible for managing the Administrator users. The Crypto officer must operate within the Security Rules and Physical Security Rules specified in Sections 3.1 and 3.2. The Crypto officer uses a secure web-based HTTPS connection to configure the Gateway. Only one Crypto Officer is defined in the Gateway. The Crypto Officer authenticates to the Gateway using a username and password.

Administrator Role: This role performs general Gateway configuration such as defining the WLAN, LAN and DHCP settings, performing self-tests and viewing system log messages for auditing purposes. No CO security functions are available to the Administrator. The Administrator can also reboot the Gateway if deemed necessary.

The Administrator must operate within the Security Rules a specified in Section 3.1 and always uses a secure web-based HTTPS connection to configure the Gateway. The Administrator authenticates to the Gateway using a username and password. Up to 5 operators who can assume the Administrator role can be defined. All Administrators are identical i.e. they have the same set of services available. The Crypto Officer is responsible for managing (creating, deleting) Administrator users.

The follow table outlines the functionalities that are provided by each role:

Categories	Features	Operator Roles											
		Crypto Officer						Administrator					
		Show[1]	Set[2]	Add[3]	Delete[4]	Zeroize[5]	Default Reset[6]	Show[7]	Set[8]	Add[9]	Delete[10]	Zeroize[11]	Default Reset[12]
System Configuration													
• General	Hostname	X	X				X	X	X				X
	Domain name	X	X				X	X	X				X
	Date/Time	X	X				X	X	X				X
• WAN	DHCP client	X	X				X	X	X				X
	Static IP address	X	X				X	X	X				X
	10/100 MBps half/full duplex/auto	X	X				X	X	X				X
• LAN	IP address	X	X				X	X	X				X
	Subnet mask	X	X				X	X	X				X
• Operating Mode	Gateway – FIPS	X	X				X	X	X				X
	Gateway – Non-FIPS	X	X				X	X	X				X
	AP / Bridging Mode – FIPS	X	X				X	X	X				X
	AP / Bridging Mode – Non-FIPS	X	X				X	X	X				X
	AP / Bridging Mode – FIPS / IPv6	X	X				X	X	X				X
	AP / Bridging Mode – Non-FIPS / IPv6	X	X				X	X	X				X
Wireless Configuration													
• General	SSID	X	X				X	X	X				X
	Channel Number	X	X				X	X	X				X
	• Enable / Disable Auto Selection	X	X				X	X	X				X
	• Auto selection button	X	X				X	X	X				X
	Transmit Power Mode	X	X				X	X	X				X
	Fixed Power Level	X	X				X	X	X				X
	Beacon Interval	X	X				X	X	X				X
	RTS Threshold	X	X				X	X	X				X
	DTIM	X	X				X	X	X				X
	Basic Rates	X	X				X	X	X				X
	Preamble	X	X				X	X	X				X

[1] *The operator can view this setting*
[2] *The operator can change this setting*
[3] *The operator can add a required input. For example: Adding an entry to the MAC address filtering table*
[4] *The operator can delete a particular entry. For example: Deleting an entry from the MAC address filtering table*
[5] *The operator can zeroize these keys.*
[6] *The operator can reset this setting to its factory default value. This is done by performing a zeroize*
[7] *The operator can view this setting*
[8] *The operator can change this setting*
[9] *The operator can add a required input. For example: Adding an entry to the MAC address filtering table*
[10] *The operator can delete a particular entry. For example: Deleting an entry from the MAC address filtering table*
[11] *The operator can zeroize these keys.*
[12] *The operator can reset this setting to its factory default value. This is done by performing a zeroize*

Categories	Features	Operator Roles											
		Crypto Officer						Administrator					
		Show[1]	Set[2]	Add[3]	Delete[4]	Zeroize[5]	Default Reset[6]	Show[7]	Set[8]	Add[9]	Delete[10]	Zeroize[11]	Default Reset[12]
	Enable / Disable Broadcast SSID	X	X				X	X	X				X
• Encryption	No Encryption	X	X				X						X
	Dynamic Key Management	X	X				X						X
	3DES	X	X			X	X						X
	AES (128-/192-256-bit)	X	X			X	X						X
• Bridging	Wireless Mode	X	X				X	X	X				X
	Spanning Tree Protocol	X	X				X	X	X				X
	Channel No	X	X				X	X	X				X
	Tx Pwr Mode	X	X				X	X	X				X
	Bridge signal strength LED port	X	X				X	X	X				X
	Add/Remove Remote AP's BSSID	X	X				X	X	X				X
• Encryption	No Encryption	X	X				X						X
	3DES	X	X		X	X	X						X
	AES (128-/192-256-bit)	X	X		X	X	X						X
• MAC Address Filtering	Enable/Disable	X	X				X	X					X
	Add/Delete entry			X	X								
	Allow/Disallow Filter	X	X				X	X					X
• Rogue AP Detection	Enable/Disable	X	X				X	X	X				X
	Known AP MAC address			X	X								
	Email / Display rogue AP	X	X				X	X	X				X
Service Settings													
• DHCP Server	Enable / Disable	X	X				X	X	X				X
	Starting / Ending IP address	X	X				X	X	X				X
• Subnet Roaming	Enable / Disable	X	X				X	X	X				X
	Coordinator Address	X	X		X		X	X	X	X			X
• Print Server	Enable/ Disable	X	X				X	X	X				X
• SNMP agent	Enable/ Disable	X	X				X	X	X				X
	Community settings	X	X				X	X	X				X
	Secure User Configuration	X	X				X	X	X				X
	System Information	X	X				X	X	X				X
User Management													
• List All Users		X		X	X		X	X					X
• Add New User			X										
• User Password Policy	Enable/Disable	X	X				X						X
	Policy setting												
Monitoring/Reports													
• System Status	Security Mode	X						X					
	Current Encryption Mode	X						X					
	Bridging encryption mode	X						X					
	System Uptime	X						X					
	Total Usable memory	X						X					
	Free Memory	X						X					
	Current Processes	X						X					
	Other Information	X						X					
	Network interface status	X						X					
• Bridging Status	Status of Layer 2 bridge devices	X						X					

Categories	Features	Operator Roles											
		Crypto Officer						Administrator					
		Show[1]	Set[2]	Add[3]	Delete[4]	Zeroize[5]	Default Reset[6]	Show[7]	Set[8]	Add[9]	Delete[10]	Zeroize[11]	Default Reset[12]
• Wireless Clients	MAC Address (manfr's name) Received Signal Strength TX rate	X X X						X X X					
• Adjacent AP List	AP MAC address SSID Channel Signal Noise Type Age WEP	X X X X X X X X						X X X X X X X X					
• DHCP Client List	Client Hostname IP Address MAC Address (manfr's name)	X X X			X X X			X X X			X X X		
• System Log	Date/Time/Message	X			X			X			X		
• Web Access Log		X			X			X			X		
• Network Activities		X			X			X			X		
System Administration													
• Firmware Upgrade		X											
• Self-Test		X						X					
• Factory Defaults		X											
• Reboot		X						X					
• Utilities	Ping Traceroute	X X						X X					

User Role: This role is assumed by the wireless client workstation that uses static or dynamic key AES or 3DES encryption to communicate wirelessly with the Gateway AP. Authentication is implicitly selected by the correct knowledge of the static key, or for dynamic key encryption, EAP-TLS authentication is performed and the client uses its public key certificate to authenticate itself. The static key (TDES or AES key) is configured on the Gateway by the Crypto officer. The static key must be pre-shared between the Gateway and User. The Gateway supports 128 Users (client workstations) if MAC address filtering is disabled. If MAC address filtering is enabled, only 60 Users are allowed.

The only service available to the User role is the ability to send data to and through the 3e-DMG. All data is sent in the form of 802.11b wireless packets. All wireless communication is encrypted using either 3DES or AES encryption (based upon Gateway configuration). In bypass mode plaintext packets can also be sent to the Gateway

Security Server Role: This role is assumed by the authentication server, which is a self-contained workstation connected to the Gateway over the Ethernet Uplink WAN port. The security server is employed for authentication of wireless clients and key management activities. The Security Server is used only during dynamic key exchange. The Security Server authenticates using a shared secret which is used as an HMAC-SHA1 key to sign messages sent to the Gateway during dynamic key exchange. The Security Server IP address and password are configured on the Gateway by the Crypto Officer. Only one Security Server is supported.

The Security Server performs following services:

a) Authenticate wireless clients for the Gateway

b) Perform a DH key exchange with the Gateway to negotiate an AES key

c) Send unicast key to the Gateway encrypted with the AES key negotiated using a DH key exchange

2.2 Authentication Mechanisms and Strength

The following table summarizes the four roles and the type of authentication supported for each role:

Role	Type of Authentication	Authentication Data
Crypto Officer	Role-based	Userid and password
Administrator	Role-based	Userid and password
User	Role-based	Static Key (TDES or AES)
User	Role-based	CA signature
Security Server	Role-based	HMAC SHA1 (Shared secret)

The following table identifies the strength of authentication for each authentication mechanism supported:

Authentication Mechanism	Strength of Mechanism
Userid and password	Minimum 6 characters => 72^6 = 1.39E11
Static Key (TDES or AES)	TDES (192-bits) or AES (128, 192, or 256-bits)
HMAC SHA-1 shared secret	Minimum 6 characters => 72^6 = 1.39E11
CA signature	128-bit

3. Secure Operation and Security Rules

In order to operate the 3e-series securely, each operator should be aware of the security rules enforced by the module and should adhere to the physical security rules and secure operation rules detailed in this section.

3.1. Security Rules

The following 3e-series security rules must be followed by the operator in order to ensure secure operation:

1. Every operator (Crypto Officer or Administrator) has a user-id. No operator will violate trust by sharing his/her password associated with the user-id with any other operator or entity.
2. The Crypto Officer will not share any key, or SRDI used by the 3e-series unit with any other operator or entity.
3. The Crypto Officer will not share any MAC address filtering information used by the 3e-series with any other operator or entity.
4. The operators will explicitly logoff by closing all secure browser sessions established with the 3e-series.
5. The operator will disable browser cookies and password storing mechanisms on the browser used for web configuration of the 3e-series unit.
6. The Crypto officer is responsible for inspecting the tamper evident seals on a daily basis. A compromised tape reveals message “OPENED” with visible red dots. Other signs of tamper include wrinkles, tears and marks on or around the label.
7. The Crypto Officer should change the default password when configuring the Gateway for the first time. The default password should not be used.

3.2. Physical Security Rules

The following section contains detailed instructions to the Crypto Officer concerning where and how to apply the tamper evident seals to the 3e-series unit enclosure, in order to provide physical security for FIPS 140-2 level 2 requirements.

Security seals were added to the back plate side of enclosure on flat of all antenna connectors. A ½” 440 Pan Head screw replaces the lower right screw on each circular connector. Then two 440 kept nuts were added and tightened together with washers facing each other 1/32” form the pem. This prevents the screws from being removed and thus entry cannot be obtained without removing the security labels.

Materials:

3e-series unit – Quantity: 1
Seal, Tape, Tamper-evident – Quantity: 3
Isopropyl Alcohol Swab
3M Adhesive Remover (citrus or petroleum based solvent)

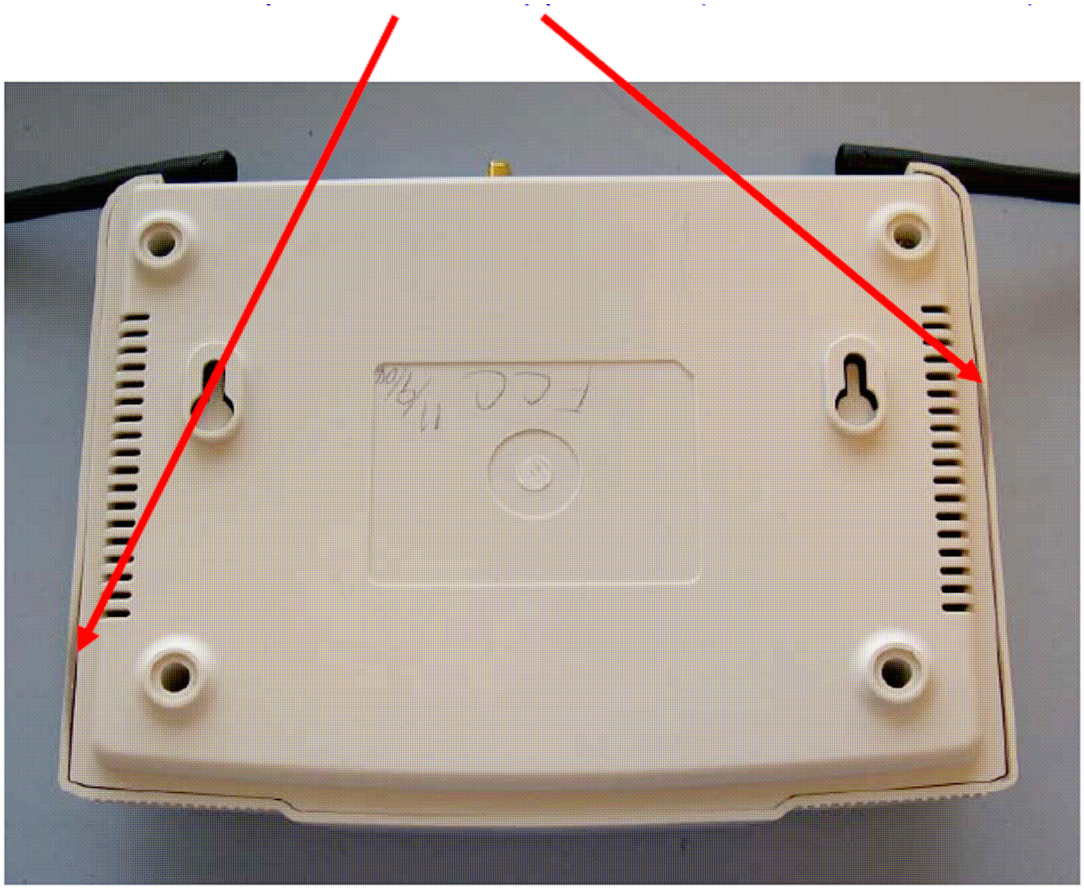
Installation – Tamper-evident tape

1. Locate on the 3e-series unit the placement locations of tamper-evident tape seals. (Tape seal locations are shown in Figure 1 and 2).
2. Thoroughly clean area where tamper-evident tape seal is to be applied with isopropyl alcohol swab. Area must be clean of all oils and foreign matter (dirt, grime, etc.)
3. Record tracking number from tamper-evident tape seal.
4. Apply seal to locations on the 3e-series units as shown in Figures 1 and 2. It is important to ensure that the seal has equal contact area with both top and bottom housings.
5. After application of seals to the Gateway, apply pressure to verify that adequate adhesion has taken place.

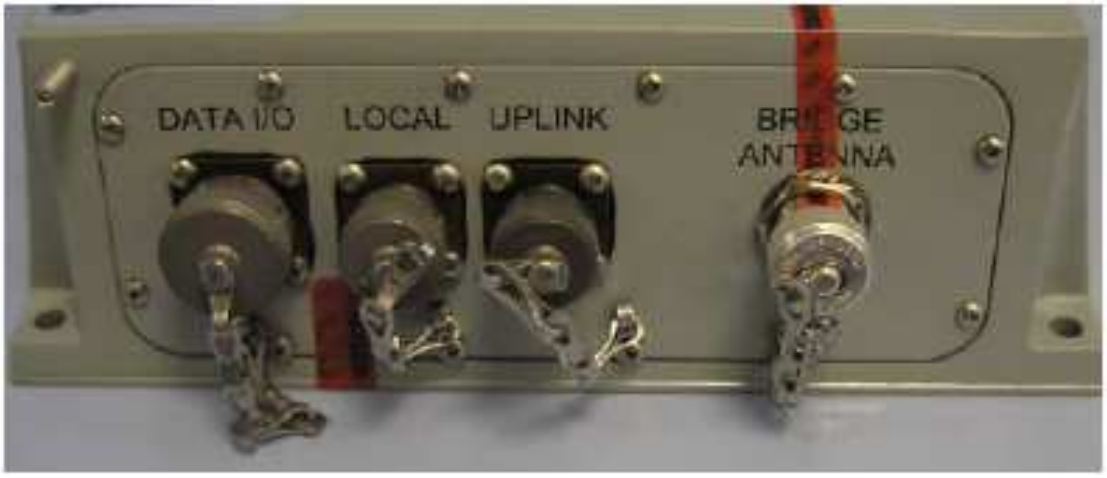
Removal – Tamper-evident tape

1. Locate on 3e-series unit the placement locations of tamper-evident tape seals. (Tape seal locations are shown in Figures 1 and 2)
2. Record tracking numbers from existing tamper-evident tape seal and verify physical condition as not tampered or destroyed after installation.
3. Cut tape along seam of 3e-series unit to allow opening of enclosure.
4. Remove nut and washer from antenna connectors.
5. Using 3M adhesive remover or equivalent, remove residual tamper-evident seal tape. (Locations are shown in Figures 1 and 2)

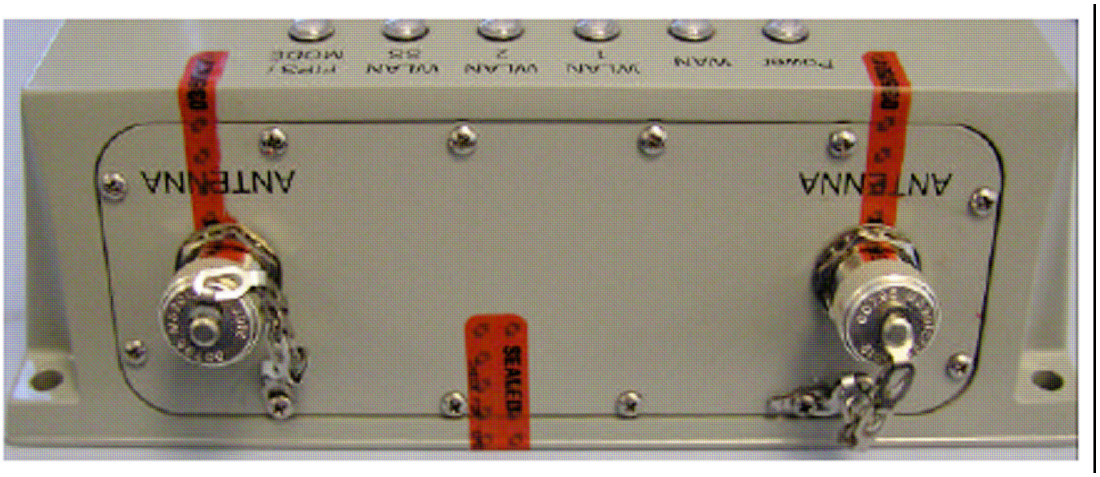
For the 3e-519, apply seal to locations as indicated by the arrows in Figures 1. Ensure that the seal has equal contact area with both top and bottom housings.



3e-519



3e-525A



3e-525A

3e-525N

3e-525N

3.3 System Administration

Firmware Upgrade

Only the Crypto Officer can select a file to upload for firmware upgrade.

Self-Tests

Both Crypto Officer and Administrators can initiate the self-test suite.

The test takes few seconds to complete. A beep will be heard at the end of the test and the result will be displayed. The self-test suite covers AES, 3DES, SHA-1, HMAC SHA-1, PRNG, Diffie Hellman for Dynamic Key Exchange, and SHA1 algorithm for firmware integrity test.

Factory Default

Only the Crypto Officer can restore the Gateway to the factory default settings. For the Gateway, a reset switch is provided on the back chassis that achieves the same goal. When this switch is depressed for 10 seconds or longer, it resets the module back to factory default settings.

Reboot

Both Crypto Officer and Administrators can reboot the Gateway.

Security Relevant Data Items

This section specifies the 3e-DMG's Security Relevant Data Items (SRDIs) as well as the access control policy enforced by the 3e-DMG.

4.1 Cryptographic Algorithms

The 3e-DMG supports the following FIPS Approved cryptographic algorithms:

- TDES (ECB, CBC modes; 192-bit keysize)
- AES (ECB mode; 128, 192, 256-bit keysizes)
- SHA-1
- HMAC-SHA1
- FIPS 186-2 (Appendix 3.1 and 3.2) PRNG

The 3e-DMG also supports the following non-FIPS cryptographic algorithms:

- Diffie Hellman (1024-bit modulus)

- RSA decrypt (PKCS#1) for key un-wrapping.
- RC4 (used in WEP)
- MD5 hashing (used in MS-CHAP for PPPoE and SNMP agent)
- DES (CBC) (used in SNMP v3)
- AES (CFB mode; 128 bit keysize) (used in SNMP v3)

4.2 Self-tests

4.2.1 Power-up Self-tests

3DES ECB - encrypt/decrypt KAT

3DES CBC - encrypt/decrypt KAT

AES ECB - encrypt/decrypt KAT

SHA-1 KAT

HMAC-SHA-1 KAT

FIPS 186-2 (Appendix 3.1, 3.3) KAT

Integrity Test for firmware

4.2.2 Conditional Self-tests

CRNGT for Approved PRNG

CRNGT for non-Approved PRNG (Open SSL based)

Bypass Test

Firmware Load Test

4.2.3 Critical Functions tests

DH pairwise consistency test (power-up)

4.3 Cryptographic Keys and SRDIs

The 3e-DMG contains the following security relevant data items:

Security Relevant Data Items	SRDI Description	Key Zero-izing
AES or 3DES Static Key	Data encryption/decryption using an AES static key (128, 192, or 256-bits) or 3DES static key (192-bits)	N/A The key is stored encrypted.
AES or 3DES Dynamic Broadcast Key	Data encryption/decryption using an internally generated AES key (128, 192, or 256-bits) or 3DES (192-bits)	Key is zero-ized on a power-cycle, CryptoOfficer changes from DKE mode to static key mode, or re-applies DKE mode.
AES or 3DES Dynamic Unicast Key	Data encryption/decryption using an dynamically exchanged AES key (128, 192, or 256-bits) or 3DES (192-bits)	Key is zero-ized on a power-cycle, CryptoOfficer changes from DKE mode to static key mode, DKE mode is re-applied, or a client disassociates.
AES Internal Key	Used to encrypt configuration file	The key can be zeroized by powering down the module and upgrading the firmware
AES Post-Authentication Key	AES Key used to decrypt the 3DES/AES Dynamic Unicast Key	The key is zeroized after the unicast key (encrypted by this AES key) is decrypted by the module.
HMAC SHA-1 Key	Key used to verify firmware integrity and authenticity during firmware upgrade	The key is zeroized by upgrading firmware twice.
HMAC SHA-1 Shared Secret	Secret used to authenticate the Security Server	N/A. The key is stored encrypted
TLS Session Key	TDES key used to encrypt/decrypt configuration sessions (via HTTPS)	This key is zeroized when the module is power cycled.
RSA Private Key	Used to decrypt pre-master key in TLS negotiation	The key is zeroized by setting the module to factory default and upgrading the firmware twice.
Crypto-officer password	CO Password	This password can be zeroized by setting the module to factory default.
Administrator password	Administrator Password	This password can be zeroized by setting the module to factory default.
HMAC SHA-1 SNMP key	This key is used to authenticate SNMP packets.	The key is zeroized by setting the module to Factory Default.

Diffie-Hellman Private exponent	This exponent is used to negotiate the AES post authentication key with the security server.	The key is zeroized after the unicast key (encrypted by the established AES key) is decrypted by the module.

4.4 Access Control Policy

The 3e-DMG maintains and enforces the access control policy for each SRDI stored within the module. These access control policies cannot be changed or modified by any role within the module. The permissions are categorized as a set of three separate permissions: read (R), write (W), execute (E). If no permission is listed, then the operator cannot access the SRDI. The following table defines the access that an operator has to each SRDI and through which services.

3e-DMG SRDI Roles and Services Access Policy	Security Relevant Data Item	AES or TDES Static Key	AES or TDES Dynamic Broadcast	AES or TDES Dynamic Unicast	AES Internal Key	AES Post-authentication Key	HMAC SHA-1 Key	HMAC SHA-1 Shared Secret	TLS Session Key	RSA Private Key	Crypto-officer password	Administrator Password	HMAC SHA-1 SNMP key
Role/Service													
Crypto-officer Role													
System Configuration					E				E	E			
Wireless Configuration		W			E			W	E	E			
Service Settings					E				E	E			W
User Management									E	E	W	W	
Monitoring/Reporting					E				E	E			
System Administration					E		E		E	E			
Administrator Role													
System Configuration					E				E	E			
Wireless Configuration					E				E	E			
Service Settings					E				E	E			W
User Management									E	E		W	
Monitoring/Reporting					E				E	E			
System Administration					E				E	E			
User Role													

Sending data		E	E	E									
Authentication Server Role													
Provides authentication				W		W		E					

5. Operational Environment

This section does not apply since the module is operated in a non-modifiable operating environment.

6. EMI/EMC

The module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e. for business use).

7. Design Assurance

3eTI implements a configuration management (CM) system for the 3e-DMG, 3e-DMG components, and associated 3e-DMG documentation. The CM infrastructure is based on the UNIX CM utility “CVS”.

8. Mitigation of Other Attacks

The module does not claim to mitigate any specific attacks.